

THE CONSEQUENCES OF INFORMATION TECHNOLOGY CONTROL WEAKNESSES ON MANAGEMENT INFORMATION SYSTEMS: THE CASE OF SARBANES OXLEY INTERNAL CONTROL REPORTS

Li, Peters, Richardson, Watson, 2012

Relationship between it controls and frs quality

- * Arguably, if there are significant weaknesses over the capturing or processing of data within the FRS, the information produced by such a system may be less effective in its ability to aid decision making.
- * Firms reporting material weaknesses in IT controls are hypothesized to have weaker controls over the production of management information, which negatively impacts the quality of the information management uses in forming earnings forecasts, thus resulting in lower forecast accuracy.

Information quality characteristics

- * Data processing integrity
 - * controls over the input of data, changes to system design, maintenance of data, and system support.
- * System access and security
 - * logical access, and segregation of duty issues, which threaten data security, as well as a lack of disaster recovery or records
- * System structure and usage
 - * decentralized and disparate systems, and weak information and communication, as well as documentation and training

Findings

- * firms reporting IT material weaknesses in internal controls from 2004 to 2008 under SOX 404
- * have significantly larger management forecast errors
 - * ITW related to data integrity has greatest impact
- * than firms reporting either effective internal controls or non-IT material weaknesses
- * improvement (deterioration) of IT controls is associated with decrease (increase) in forecast errors

IT internal control weaknesses and Firm performance: An organizational liability lens

Stoel & Muhanna (2011)

Interdependence between it controls and business operations

- * Controls needed for protection of:
 - * Confidentiality
 - * Integrity
 - * Accessibility
- * Research aims at providing direct empirical evidence regarding the performance impact of shortcomings in the firm's IT internal controls, **irrespective** of the public disclosure of specific possible manifestations (e.g., breach) of those shortcomings.

Findings

- * we examine the linkage between IT internal control quality and current performance, measured using contemporaneous return on assets (ROA).
 - * Firms with reported material IT ICWs deliver lower ROA
 - * Firms that report an IT ICW have lower accounting earnings compared to firms with strong IT internal controls. We also find that IT ICW moderates the association between accounting earnings and market valuation, with firms reporting weak IT internal controls having a lower earnings multiple.
- * Does the market price in IT ICW's?
 - * We find no direct effect of IT internal control quality on market valuation; however, we do find that IT internal control quality negatively moderates the association between accounting earnings and market valuation.

Information Security and Sarbanes- Oxley

Compliance: An Exploratory Study

Wallace, Lin, and Cefaratti (2011)

Frameworks

- * While COSO and COBIT outline requirements for various security structures and controls
- * ISO 17799 provides the details on how to develop and implement these components
- * COBIT suggests to organizations how they should monitor and control but is not very detailed in terms of providing guidelines for how to implement security to achieve control

ISO

1. Security Policy
2. Organizational Security
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Systems Development and Maintenance
9. Business Continuity Management
10. Compliance

* In all there are 124 recommended IT controls

Participants

- * The majority of the participants had some type of professional certification.
- * The most common certifications were:
 - * Certified Internal Auditor (CIA)
 - * Certified Public Accountant (CPA)
 - * Certified Information Systems Auditor (CISA)

Findings

- * Controls such as deploying antivirus software and authenticating remote users accessing the network were ranked as the most commonly implemented controls.
- * Protecting equipment from unauthorized access and tracking the location of removable computer media using IT were ranked as the least commonly implemented controls.
- * See table 4 and 5

“Not Sure” Findings

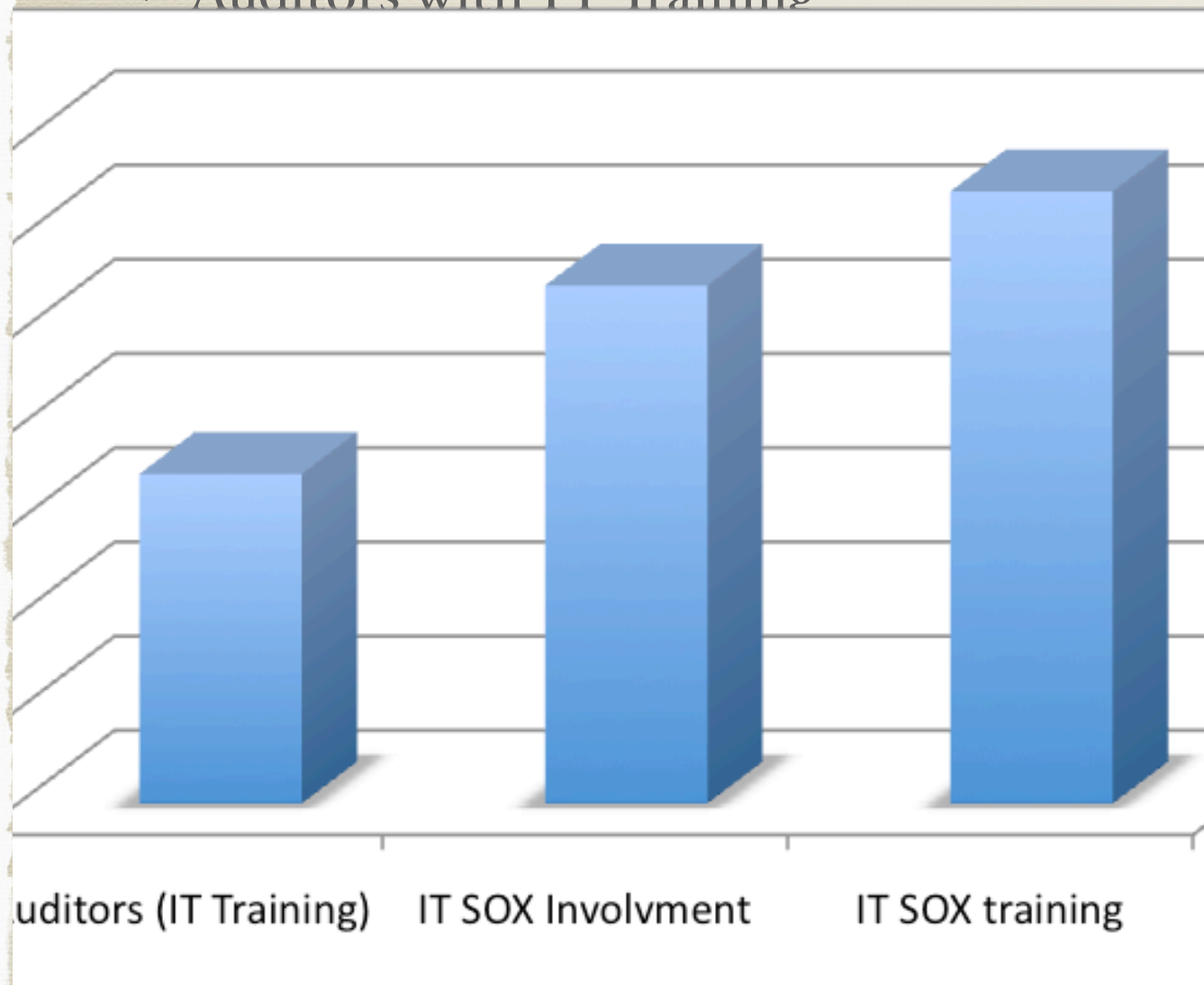
TABLE 7
Controls Most Frequently Listed as “Not Sure”

| ISO # | Control Description | Frequency of “Not Sure” Responses |
|--------------|--|--|
| 9.4.8 | Our organization uses IT to deploy routing controls requiring origin and destination address checking. | 208 |
| 8.2.1 | Our organization uses IT to monitor power capacity demands. | 175 |
| 8.4.3 | Our organization uses IT to analyze fault logs for trends. | 175 |
| 12.3.2 | Our organization uses IT to record each use of software audit tools. | 169 |
| 9.5.1 | Our organization uses IT to deploy automatic terminal identification to authenticate connections. | 169 |
| 9.5.8 | Our organization uses IT to limit connection time for high-risk applications. | 166 |
| 8.7.7 | Our organization uses IT to protect information that is exchanged using voice and video outputs. | 165 |
| 8.6.1 | Our organization uses IT to track the location of removable computer media. | 164 |
| 9.4.5 | Our organization uses IT to control access to diagnostic ports. | 159 |
| 8.1.6 | Our organization uses IT to measure security compliance at a third-party facility. | 157 |
| 8.4.3 | Our organization uses IT to maintain a fault log. | 157 |

- CPA’s selected “not sure” more frequently than non-CPA’s
- CISA’s selected “not sure” less frequently than non-CISA’s
- What Is ISO Category 8? 9?

Training

* Auditors with IT Training



- Auditors with IT Training
 - 35 more controls were likely to be implemented
- IT employees participate in SOX Compliance
 - 55 more controls were likely to be implemented
- IT personnel received SOX compliance training
 - 65 more controls were likely to be implemented

SOX 404 Reported Internal Control Weaknesses: A TEST of COSO Framework Components and Information Technology

Klamm and Watson (2009)

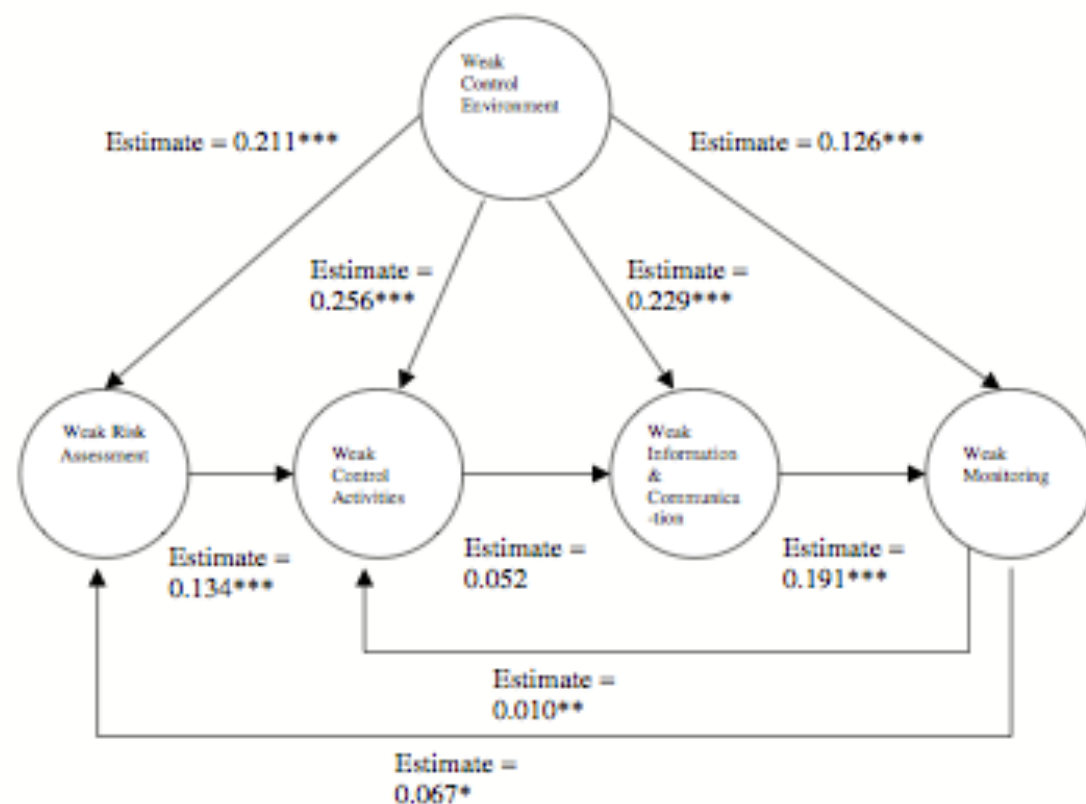
Purpose of study

- * Examines interrelatedness of COSO components
- * Examines impact of IT MW's on COSO components

Results

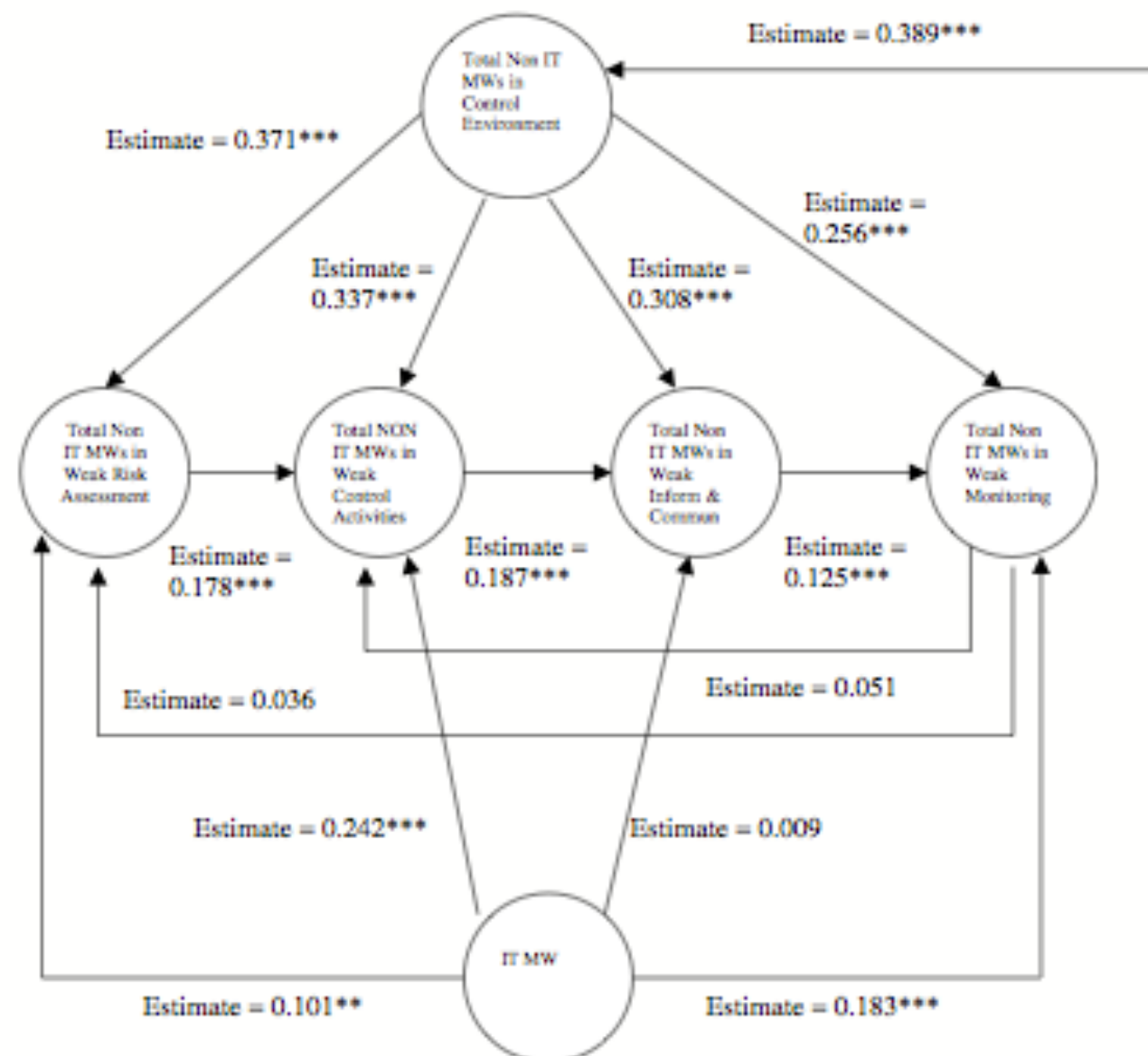
- * Multivariate analysis shows that a weak control environment is positively related to weak risk assessment, control activities, information and communication, and monitoring components. Also, a weak risk assessment component is positively related to a weak control activities component; MWs in the control activities component are positively related to MWs in the information and communication component; and a weak information and communication component is positively related to a weak monitoring component
- * IT-Weak firms report a greater scope of internal control problems, i.e., internal control problems that involve multiple COSO components, as well as a greater negative effect for the existence of an IT internal control problem in selected COSO components. We find evidence that weak IT control environment, risk assessment, and control activities decrease financial reporting reliability.
- * IT-Weak firms also have more non-IT related MWs, misstatements, and weak COSO components

FIGURE 1
Structural Equation Model
Interrelatedness of the COSO Framework Components*



Chi-square divided by the degrees of freedom (CMIN/DF) 5.8530
Comparative Fit Index (CFI) 0.9680
Root Mean Square Error of Approximation (RMSEA) 0.0996

FIGURE 2
Structural Equation Model
The Impact of Information Technology Material Weaknesses on Non-IT Material Weaknesses*



Chi-square divided by the degrees of freedom (CMIN/DF) 1.0293
Comparative Fit Index (CFI) 1.0000
Root Mean Square Error of Approximation (RMSEA) 0.0077

The effect of IT controls on financial reporting

Grant, Miller & Alali (2008)

What Standards does paper use for support?

- * How are these standards used? What do they say (not say) about IT controls?
 - * SAS 94
 - * “The nature and character of an entity’s use of technology in its information system affects the entity’s overall internal control structure”
 - * SOX
 - * PCAOB AS #5
 - * an IC deficiency occurs when the design or operation of the control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis
 - * IT general controls could have an effect on the operating effectiveness of other controls and requires auditors to provide an opinion on the effectiveness of internal controls over financial reporting.
 - * General Controls – Insure Proper Operations
 - * Application Controls – Processing & Storage of Information

IT Deficiencies Examined in Study?

- * IT deficiencies include controls related to
 - * software programs
 - * program implementations
 - * segregation of duties associated with access to computer accounting or financial reporting records
 - * problems with access to electronic data and programs
- * What other controls might be important for accounting/auditing?
- * Why weren't they investigated?

Findings

- * These IT deficiencies include controls related to software programs, program implementations, segregation of duties associated with access to computer accounting or financial reporting records, and problems with access to electronic data and programs
- * IC deficiencies and accounting errors occur more often in companies when IT deficiencies exist. Accounting issues dealing with revenue recognition; receivables, investments, and cash; inventory, vendor, and cost of sales; and financial statement, footnote, US GAAP, and segment disclosures issues are more widespread in companies that report IT deficiencies. When compared to companies that do not report IT deficiencies, IT deficient companies pay higher audit fees, while employing smaller audit firms. In addition, companies that report IT deficiencies are smaller, based on revenues, than companies that do not report IT deficiencies.

CF Disclosure Guidance #2

October, 2011

What is this?

- This guidance provides the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents.
- It is NOT a rule, regulation, or statement of the SEC

Why

- Costs and Consequences:
 - Remediation Costs
 - IT security control costs
 - Lost Revenue
 - Litigation Costs
 - Reputational damage

Disclosures (Risk Factors)

- Company should disclose risk if they make an investment in the company speculative or risky.
 - prior cyber incidents and the severity and frequency of those incidents.
 - the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption.
 - How adequate are IT security controls to prevent these risks
 - But.. “registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk factor disclosure”
- Appropriate Disclosures:
 - Discussion of aspects of the registrant’s business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
 - To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
 - Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
 - Risks related to cyber incidents that may remain undetected for an extended period; and
 - Description of relevant insurance coverage.
- But...
 - “While registrants should provide disclosure tailored to their particular circumstances and avoid generic “boilerplate” disclosure, we reiterate that the federal securities laws do not require disclosure that itself would compromise a registrant’s cybersecurity. Instead, registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence.”

Disclosures (MD&A)

“ Registrants should address cybersecurity risks and cyber incidents in their MD&A if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant’s results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.”

Other Disclosures

- Description of Business
 - If cyber incident materially effects:
 - products, services, relationships with customers or suppliers, or competitive conditions
- Legal Proceedings
 - If material leading proceedings in which company is a party

Impact on Financial Statement (after incident)

- “Cyber incidents may result in losses from asserted and unasserted claims, including those related to warranties, breach of contract, product recall and replacement, and indemnification of counterparty losses from their remediation efforts.”
- “Cyber incidents may also result in diminished future cash flows, thereby requiring consideration of impairment of certain assets including goodwill, customer-related intangible assets, trademarks, patents, capitalized software or other long-lived assets associated with hardware or software, and inventory.

Material, Material, ...

“Securities Act Rule 408, Exchange Act Rule 12b-20, and Exchange Act Rule 14a-9.

Information is considered material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would significantly alter the total mix of information made available.”

Cyber Attacks Abound Yet Companies Tell SEC Losses are Few

By Chris Strohm, Eric Engleman and Dave Michaels - Apr 3, 2013

What is the article about?

Updates

- <http://www.bloomberg.com/news/2013-04-10/sec-urged-to-give-stronger-guidance-on-cyber-disclosure.html>
- Senator Nelson Rockefeller*
 - Labeled current SEC guidance insufficient
 - “Investors deserve to know whether companies are effectively addressing their cybersecurity risks -- just as investors should know whether companies are managing their financial and operational risks,”
- Lona Nallengara, the SEC’s corporation finance director
 - “If you’re an investor and you want to see the company you are investing in is adequately protected against cyber attack, you’d want to know did their systems detect it?” Nallengara said. “Did they know they got breached? Or did they find out a month later when someone told them that we found records this came from your company?”

SEC Updates

- S.E.C. Chairman Mary Jo White
 - (May 1, 2013) asked her staff to give her “a briefing of the current disclosure practices and overall compliance” with SEC guidance on cybersecurity and “any recommendations they have regarding further action in this area,”
- Senator Nelson Rockefeller
 - White’s response “makes it clear the SEC will continue to prioritize increased disclosure of cybersecurity practices and to monitor the steps companies are taking to manage cybersecurity risks”

Cybersecurity Roundtable

March 26th, 2014

Opening Statement

- Chair, Mary Jo White
 - “Cyber threats are of extraordinary and long-term seriousness.”
 - The SEC’s formal jurisdiction over cybersecurity is directly focused on the integrity of our market systems, customer data protection, and disclosure of material information.
 - in October 2011, our Division of Corporation Finance issued guidance on existing disclosure obligations related to cybersecurity risks and incidents to assist public companies in framing disclosures of cybersecurity issues. That guidance makes clear that material information regarding cybersecurity risks and cyber incidents is required to be disclosed.

Proposed Regulations

- Security Exchanges (NASDAQ); Security Associations (NASD); Futures Exchanges (CME); Clearing Agencies;
 - require an entity covered by the rule to test its automated systems for vulnerabilities, test its business continuity and disaster recovery plans, notify the Commission of cyber intrusions, and recover its clearing and trading operations within specified time frames.
- Registered investment advisers, broker-dealers, and funds, including
 - data protection and identity theft vulnerabilities

Opening Statement

- Commissioner Luis A. Aguilar
 - “I have become particularly concerned about the risks that cyber-attacks pose to public companies, and to the capital markets and its critical participants, including the exchanges, clearing agencies, transfer agents, broker-dealers, and investment advisers. Cyber-attacks aimed at these market participants can have devastating effects on our economy, on individual consumers, and on the markets and investors that the SEC was created to safeguard.”
 - “...in 2011 the staff issued guidance to public companies about their disclosure obligations with respect to cybersecurity risks and cyber incidents... However, the increased pervasiveness and seriousness of the cybersecurity threat raises questions about whether more should be done to ensure the proper functioning of the capital markets and the protection of investors.”

SEC Office of Compliance Inspections and Examinations (OCIE)

Cybersecurity Initiative
April 15, 2014

Security Industry

- OCIE's cybersecurity initiative is designed to assess cybersecurity preparedness in the securities industry and to obtain information about the industry's recent experiences with certain types of cyber threats.
- Examination of 50 registered broker-dealers and registered investment advisors

What will be examined?

1. the entity's cybersecurity governance
2. identification and assessment of cybersecurity risks,
3. protection of networks and information,
4. risks associated with remote customer access and funds transfer requests,
5. risks associated with vendors and other third parties,
6. detection of unauthorized activity,
7. experiences with certain cybersecurity threats.

Review the types of questions firms will be asked to provide answer for:

- Could you assist with a compliance request made by one a firm undergoing such an examination?